

## DESCRIPTION

### MOBILE COMMUNICATION SYSTEM, BASE STATION, AND HSDPA TRANSMISSION METHOD USED IN THEM

5

#### Technical Field

[0001] The present invention relates to a mobile communication system, a base station, and an HSDPA (High Speed Downlink Packet Access) transmission method. In particular, the present invention relates to ciphering for a radio bearer 10 on an RLC (Radio Link Control) transparent type transfer mode in the HSDPA transmission method.

#### Background Art

[0002] Typically in a DCH (Dedicated Channel), synchronization at a transport 15 channel level is set up between a mobile station (UE: user equipment) and a UTRAN (Universal Terrestrial Radio Access Network), and its transmission timing is transmitted by timing called CFN (Connection Frame Number).

[0003] In a radio bearer on RLC-TM (Radio Link Control – Transparent Mode), a MAC (Medium Access Control) – d protocol conducts ciphering as shown in FIG. 20 4 and the CFN is used in a COUNT-C which is used in ciphering calculation.

[0004] Ciphering is executed in RLC\_AM and RLC UM protocols on radio bearers on RLC\_AM (Radio Link Control – Acknowledged Mode) and RLC UM (Radio Link Control – Unacknowledged Mode).

[0005] On the other hand, basically in the HSDPA, one physical channel is used in 25 common by a plurality of User Equipments in a time division manner, and scheduling for actually conducting radio communication is conducted in a base station (see, for example, Non-Patent Document 1).

[0006] Non-Patent Document 1: "High Speed Downlink Packet Access (HSDPA); Overall description; Stage 2" [3GPP (3rd Generation Partnership Project) TS25.308 V6.0.0 (2003-12)]

5 Disclosure of the Invention

Problem to be Solved by the Invention

[0007] In the above described HSDPA transmission method, the CFN cannot be applied as actual data transmission timing. This results in a problem that ciphering cannot be executed on radio bearers (such as circuit switched calls) on the

10 RLC-TM.

[0008] In the case where the HSDPA transmission method is applied to a mobile communication network of IMT (International Mobile Telecommunications) – 2000, therefore, it is necessary to divide and assign radio resources, such as downlink channelization codes and downlink power, to resources for non-HSDPA used by radio bearers (such as circuit switched calls) in the RLC-TM and resources for the HSDPA used by radio bearers (such as packet calls) other than the RLC-TM. However, the above-described mobile communication network has a problem that a division loss in radio resources is caused and consequently radio resources cannot be used to the full.

20 [0009] Therefore, an object of the present invention is to solve the above-described problem and provide a mobile communication system in which the HSDPA can be applied to radio bearers in the RLC-TM, such as circuit switched calls, as well and the radio capacity can be used to the full, a base station, and an HSDPA transmission method used in them.

25

Means for Solving the Problem

[0010] A mobile communication system according to the present system is a

mobile communication system using the HSDPA in which one physical channel is used by a plurality of mobile stations in common in a time division form and scheduling for executing radio transmission on the physical channel is conducted by a base station, wherein the base station has a ciphering function for preventing control signals and user information directed to the mobile station from being intercepted illegally in a radio section.

[0011] A base station according to the present invention is a base station included in a mobile communication system using HSDPA in which one physical channel is used in common by a plurality of mobile stations in a time division form, wherein the base station conducts scheduling to execute radio transmission on the physical channel, and the base station has a ciphering function for preventing control signals and user information directed to the mobile station from being intercepted illegally in a radio section.

[0012] An HSDPA transmission method according to the present invention is an HSDPA transmission method using HSDPA in which one physical channel is used by a plurality of mobile stations in common in a time division form and scheduling for executing radio transmission on the physical channel is conducted by a base station, wherein the base station side executes a ciphering process for preventing control signals and user information directed to the mobile station from being intercepted illegally in a radio section.

#### Effect of the Invention

[0013] Owing to configurations and operations described hereafter, the present invention brings about an effect that the HSDPA can be applied to radio bearers in the RLC-TM, such as circuit switched calls, as well and the radio capacity can be used to the full.

### Brief Description of the Drawings

[0014] FIG. 1 is a block diagram showing a configuration of a mobile communication system according to an embodiment of the present invention;

FIG. 2 is a block diagram showing an internal configuration of a base station shown in FIG. 1;

FIG. 3 is a sequence chart showing an operation sequence between nodes in a mobile communication system according to an embodiment of the present invention;

FIG. 4 is a diagram showing a ciphering counter (COUNT-C) defined in the 3GPP; and

FIG. 5 is a diagram showing a ciphering counter (COUNT-C) according to an embodiment of the present invention.

### Description of Reference Numerals

15 [0015]

1: Mobile station (UE: user equipment)

2: Base station (node B)

3: Base station controller (RNC: radio network controller)

4: Mobile switching center (CN: core network)

20 21: Ciphering function unit

22: Radio modulator

23: Call controller

24: Scheduler

25 Best Mode for Carrying Out the Invention

[0016] In a mobile communication system according to the present invention, a base station which actually conducts scheduling in a mobile system of IMT

(International Mobile Telecommunications) using the HSDPA (High Speed Downlink Packet Access) executes ciphering on radio bearers in the RLC-TM (Radio Link Control – Transparent Mode).

[0017] In this case, ciphering is processing for preventing control signals and user information from being intercepted illegally in a radio section. Ciphering is executed by encrypting the control signals and user information by means of the ciphering key for each user and an algorithm for ciphering.

[0018] A base station controller notifies the base station of ciphering parameters (the ciphering key, START, a ciphering algorithm, ciphering execution timing) when executing ciphering. The base station initializes an HFN (Hyper Frame Number) formed of high-order bits in the COUNT-C on the basis of START, and combines a present SFN (Cell System Frame Number counter) to construct the ciphering counter (COUNT-C). The base station executes ciphering on radio bearers in the RLC-TM after ciphering execution timing.

[0019] In a mobile communication system according to the present invention, the HSDPA can also be applied to radio bearers (such as circuit switched calls) using the RLC-TM as radio bearers in a mobile communication system of IMT-2000 using the HSDPA.

[0020] In a conventional mobile communication system of IMT-2000 using the HSDPA, only a base station controller (RNC: radio network controller) is equipped with a ciphering function. In the present configuration, however, ciphering cannot be executed on RLC-TM radio bearers in the HSDPA scheme as described in the Non-Patent Document 1.

[0021] Here, the HSDPA transmission method is a radio scheme introduced to increase the downlink peak transmission rate, reduce the delay, and increase the throughput as faster an IMT-2000 transmission scheme.

[0022] To be more concrete, it becomes possible in the mobile communication

system according to the present invention to apply the HSDPA to RLC-TM radio bearers as well by mounting a ciphering function unit on a base station (node B). The base station controller transmits a signal for giving notice of information concerning ciphering to the base station. As a result, it becomes possible on the 5 base station side to execute the ciphering.

[0023] Since the ciphering counter (COUNT-C) defined in the 3GPP is formed of the HFN and the CFN (Connection Frame Number), it cannot be applied to the HSDPA system.

[0024] On the other hand, in the mobile communication system according to the 10 present invention, the COUNT-C is formed of the SFN and the HFN. As a result, it becomes possible on the base station side as well to conduct ciphering.

[0025] Here, in the case of the RLC-TM, the COUNT-C is formed of the 8-bit CFN and the 24-bit MAC-d HFN. The HFN is incremented at the CFN periods. The COUNT-C is used together with the ciphering key and an algorithm kind in 15 ciphering calculation.

[0026] The CFN is used as a frame counter at the Layer 2/ transport channel level between a mobile station (UE: user equipment) and a UTRAN (Universal Terrestrial Radio Access Network). The CFN is in the range of 0 to 255 frames [“Synchronization in UTRAN Stage 2” (3GPP TS25.402 V.6.0.0 (2003-12)] 20 (hereafter referred to as reference document 1).

[0027] The SFN deviates from the BFN [(Node B Frame Number (counter))] by T\_cells, and it is used for paging and scheduling of broadcast information. The SFN is in the range of 0 to 4095 frames (see reference document 1).

[0028] An RLC (Radio Link Control) layer provides data transfer services in three 25 modes, i.e., the RLC-AM (RLC-Acknowledged Mode), the RLC-UM (RLC-Unacknowledged Mode) and the RLC-TM to upper layers [“Radio Link Control (RLC) protocol specification”(3GPP TS25.322 V6.0.0) (2003-12)]

(hereafter referred to as reference document 2).

[0029] As was described above, in the mobile communication system according to the present invention, it becomes possible to apply the HSDPA to all radio bearers by making possible for radio bearers in the RLC-TM as well to conduct ciphering.

5 [0030] In the mobile communication system according to the present invention, the HSDPA is made applicable to all bearers. As a result, it becomes unnecessary to divide downlink channelization codes and downlink power, which are radio resources, to resources for the HSDPA and resources for non-HSDPA. Therefore, it becomes possible to use radio resources for the HSDPA to the full.

10

#### Embodiment

[0031] An embodiment of the present invention will now be described with reference to the drawings. FIG. 1 is a block diagram showing a configuration of a mobile communication system according to an embodiment of the present

15 invention. In FIG. 1, a mobile communication system according to an embodiment of the present invention includes a mobile station (UE: user equipment) 1, a base station (node B) 2, a base station controller (RNC: radio network controller) 3, and a mobile switching center (CN: core network) 4. The base station 2 is provided a ciphering function unit 21.

20 [0032] FIG. 2 is a block diagram showing an internal configuration of the base station 2 shown in FIG. 1. In FIG. 2, the base station 2 is formed of the ciphering function unit 21, a radio modulator 22, a call controller 23, and a scheduler 24.

[0033] The call controller 23 terminates control signals, such as NBAP (Node B Application Part) and ALCAP (Access Link Control Application Protocol), and exercises control on the scheduler 24, the ciphering function unit 21 and the radio modulator 22.

[0034] The scheduler 24 conducts scheduling of time division in downlink user

data transfer. The ciphering controller 21 executes ciphering on data scheduled in the scheduler 24 on the basis of ciphering control information supplied from the call controller 23, and transmits resultant data to the radio modulator 22. The radio modulator 22 conducts radio modulation, and transmits data to the mobile station 1.

[0035] Here, ciphering is processing for preventing control signals and user information from being intercepted illegally in a radio section. The ciphering is executed by encrypting the control signal and user information by the use of the ciphering key for each user and an algorithm for ciphering.

[0036] FIG. 3 is a sequence chart showing an operation sequence between nodes in a mobile communication system according to an embodiment of the present invention. FIG. 4 is a diagram showing a ciphering counter (COUNT-C) defined in the 3GPP. FIG. 5 is a diagram showing the ciphering counter (COUNT-C) according to an embodiment of the present invention. Operation conducted between nodes in a mobile communication system according to an embodiment of the present invention will now be described with reference to FIGs. 1 to 5.

[0037] In radio transmission using the HSDPA scheme according to an embodiment of the present invention, the ciphering controller 21 in the base station 2 executes ciphering on radio bearers using the RLC-TM (Radio Link Control – Transparent Mode).

[0038] Basically in the HSDPA, a plurality of mobile stations use a single channel in common by means of time division. The base station conducts scheduling for actually conducting radio transmission.

[0039] Operation conducted in the present embodiment will now be described by taking ciphering control exercised when setting up a circuit switched call as an example with reference to FIG. 3. Typically, ciphering control is already started when DCCH (Dedicated Control Channel) (signaling connection) is set up between

the mobile station 1 and the mobile switching center 4 before circuit switching is set up.

[0040] In other words, the case where ciphering is already executed as to DCCH is supposed. Furthermore, it is supposed that DCCH is set up on HS-DSCH (High

5 Speed – Downlink Shared Channel).

[0041] Since DCCH uses RLC-UM (RLC-Unacknowledged Mode) and RLC-AM (RLC-Acknowledged Mode), ciphering is conducted by the RLC-UM and RLC-AM entities on the base station controller 3 side as in the conventional scheme.

10 [0042] With reference to FIG. 3, when setting up a circuit switched call, the mobile switching center 4 issues a RAB setup request for the circuit switched call to the base station controller 3 by using RANAP (Radio Access Network Application Part): RAB (Radio Access Bearer) Assignment Request protocols (A1 in FIG. 3).

[0043] The base station controller 3 decides to map the circuit switched call onto

15 HS-DSCH. The base station controller 3 notifies the base station 2 of information concerning HS-DSCH suitable for setting up RAB, by using NBAP: RL (Radio Link) Reconfiguration Prepare (A2 in FIG. 3). The base station 2 returns its reply by using RL Reconfiguration Ready (A3 in FIG. 3).

[0044] Thereafter, the base station controller 3 executes setup of DCH (Dedicated Channel) transport bearers for uplink and HS-DSCH transport bearers for downlink according to an ALCAP procedure (A4 and A5 in FIG. 3).

[0045] After preparation within the network is completed, the base station controller 3 transmits an RRC (Radio Resource Control): Radio Bearer Setup message to the mobile station 1 to notify the mobile station 1 of information concerning HS-DSCH for setting up the circuit switching bearer (A7 in FIG. 3).

25 At the same time, the base station controller 3 transmits RL Reconfiguration Commit to the base station 2 to notify the base station 2 of timing for applying new

setting (A6 in FIG. 3).

[0046] Thereafter, the mobile station 1 sets ciphering execution timing (COUNT-C Activation Time) for applying ciphering and the ciphering counter initial value (START), and notifies the base station controller 3 of them by using an RRC: Radio Bearer Setup Complete message (A8 in FIG. 3). Operation described so far is operation prescribed in the ordinary 3GPP.

[0047] In the present embodiment, the base station controller 3 transmits a “ciphering start” message to the base station 2 in order to cause ciphering to be start to notify the base station 2 of ciphering execution timing (COUNT-C Activation Time), the ciphering counter initial value (START), the ciphering key and the ciphering algorithm (A9 in FIG. 3). Thereafter, the base station controller 3 returns a RANAP: RAB Assignment Response to the mobile switching center 4 (A10 in FIG. 3).

[0048] The call controller 23 in the base station 2 orders the ciphering function unit 21 to execute ciphering by using the ciphering parameters notified of by the base station controller 3. The ciphering function unit 21 executes ciphering on downlink data of RLC-TM radio bearers transmitted from the scheduler 24, and conducts transmission to the radio modulator 22.

[0049] In the ciphering control, the ciphering counter (COUNT-C) is used as an input of ciphering calculation. Since the ciphering counter (COUNT-C) for the RLC-TM includes the HFN (Hyper Frame Number) and the CFN (Connection Frame Number) as shown in FIG. 4, however, the ciphering counter cannot be applied to the HSDPA in which the base station 2 conducts scheduling, as it is.

[0050] In the present embodiment, the CFN is not used, but the SFN (Cell System Frame Number counter) is used as shown in FIG. 5. In other words, 12 bits included in 32 bits for the COUNT-C form the SFN and the remaining 20 bits form the HFN. The HFN is initialized by the ciphering counter initial value (START),

and then incremented at SFN periods. By the way, it is necessary in the mobile station side 1 as well to conduct decryption for ciphering after radio demodulation.

[0051] Thus, in the present embodiment, the HSDPA can be applied to radio bearers in the RLC-TM, such as circuit switched calls, as well by executing the 5 ciphering function to the RLC-TM bearers when applying the HSDPA to the base station 2.

[0052] Furthermore, in the present embodiment, the HSDPA scheme can be applied to all bearers. Therefore, it becomes unnecessary to divide and assign the radio resources (channelization codes and power) to the HSDPA (such as packet 10 calls) and the non-HSDPA (such as circuit switched calls), and the HSDPA can be applied to all radio bearers. Therefore, the radio capacity can be used to the full.